Требования законодательства и нормативной базы

написано Александр Астахов | 10 июня, 2023

Незнание закона не освобождает от ответственности.
А вот знание нередко освобождает.

Станислав Ежи Лец, польский писатель

Организации все чаще сталкиваются с необходимостью обеспечения соответствия широкому диапазону законодательных и нормативных требований, оказывающих влияние на их процессы управления информацией. Требования законодательной и нормативной базы настолько разнообразны, что мы могли бы посвятить этой теме целую главу, если бы это не уводило нас немного в сторону от основной темы. Требования эти так важны для организаций, особенно для государственных, что порой складывается впечатление, будто вся деятельность специалистов, отвечающих за безопасность этих организаций сводится к удовлетворению требований ФСТЭК, ФСБ, Министерства обороны и Банка России в области защиты информации, что выражается в прохождении проверок и получении от этих организаций соответствующих документов подтверждающих соответствие. Такие специалисты либо считают, что основная опасность для их бизнеса исходит именно от государства и заключается в возможности применения в отношении них определенных санкций, либо они уверенны что кто-то «наверху» уже оценил все риски информационной безопасности и подготовил для них универсальные рецепты в виде нормативных документов, следование которым обеспечивает достаточную защиту. Как бы наивно ни выглядели подобные рассуждения, они достаточно широко распространены, судя потому, что преобладающая часть российского рынка информационной безопасности «не выходит за рамки» нормативных требований, посвящая себя обеспечению соответствия этим требованиям не в дополнение, а вместо управления рисками.

Для того чтобы разобраться с непрерывно возрастающим количеством законодательных и нормативных инструментов регулирования, требуется определенная структуризация.

Для государства существует довольно много побудительных причин регулирования сферы информационной безопасности:

Национальная безопасность. Забота о национальной безопасности вызвана возрастанием угрозы глобального терроризма и кибертерроризма.

Обеспечение защиты государственных тайн и государственных интересов в информационной сфере.

Корпоративное управление. Государственное законодательное регулирование в сфере корпоративного управления является результатом резких провалов в области корпоративного управления, предоставления компаниями недостоверной информации о своей деятельности инвесторам, аналитикам, рейтинговым агентствам и государству.

Электронная коммерция. Регулирование в сфере электронной коммерции является результатом необходимости установления доверия к онлайновой торговле в Интернет.

Защита персональных данных. Необходимость обеспечения безопасности персональных данных является результатом очевидных упущений в области корпоративной безопасности, которые порождают утечки персональных данных.

Защита интеллектуальной собственности. Для нормального развития экономики, особенно инновационной, необходимо обеспечить защиту авторских и патентных прав, «ноу хау» и других объектов интеллектуальной собственности.

Гражданская и уголовная законодательная база, необходимая для борьбы с преступлениями в информационной сфере.

Нормативная база, специфичная для конкретного сектора (отрасли) экономики, например, электроэнергетики, газовой

отрасли и т.п.

Помимо перечисленного, другими побудительными причинами могут выступать охрана здоровья и обеспечение безопасности личности, забота о сотрудниках и клиентах, являющихся инвалидами, необходимость защиты государственных налоговых сборов, необходимость исключения дискриминации на работе и т.п.

Такое законодательство и нормативная база предназначены для того, чтобы гарантировать, что организации внедряют эффективные механизмы контроля и аудита потоков информации (персональной, финансовой и операционной). Большинство законодательных и нормативных актов рассматривают оценку рисков в качестве важного элемента этих эффективных механизмов контроля.

Не все из перечисленного в настоящее время имеет отношение к России, однако мы посмотрим на законодательство немного шире, т.к. новые нормативные акты, внедряемые на Западе, постепенно доходят и до России, хотя и в несколько искаженном виде.

Действующее информационное законодательство Российской Федерации представлено целым блоком нормативно-правовых актов самого различного уровня, начиная с Конституции, Гражданского, Уголовного и Административного кодекса РФ и заканчивая узкоспециализированными, фундаментальными источниками, регулирующими вопросы защиты информации, к которым относятся законы РФ «Об информации, информатизации и защите информации», «Об участии в международном информационном обмене», Закон о коммерческой тайне, Законы о персональных данных и о служебной информации. Перечень законодательных и нормативных актов РФ в области защиты информации приведен в Приложении № 9.

Остановимся на перечисленных группах законодательных актов более подробно, используя в качестве примеров законодательные базы Европы и Северной Америки, как наиболее развитые, а также российское законодательство, как наиболее нам близкое.

Национальная безопасность

Меры по обеспечению национальной безопасности направлены на защиту от угроз в отношении критической национальной инфраструктуры, исходящих из таких источников, как террористы, кибер-атаки и кибер-шпионаж, спонсируемые на государственном уровне, а также катастрофы техногенного, антропогенного или природного происхождения.

Европейские меры в этой области имеют тенденцию к тому, чтобы, по возможности, не использовать законодательных инструментов. Большинство правительств имеют агентства, задачей которых является защита критической национальной информационной инфраструктуры (такие как Координационный центр безопасности сетевой инфраструктуры (NISCC) в Объединенном Королевстве). В 2004 году ЕС основал Европейское Агентство по безопасности сетевой информации (ENISA).

США наделили Департамент Национальной Безопасности (DHS) всей полнотой ответственности за защиту критической национальной инфраструктуры, а также внедрили большое количество законодательных инструментов, возложив ответственность за определенные аспекты этой задачи на промышленные организации и правительственные агентства, включая Североамериканский Совет по электрической безопасности, Федеральную Комиссию по регулированию в области энергетики и др. В числе основных законодательных актов в данной области можно отметить Федеральный Акт об управлении информационной безопасностью (FISMA) и Акт США о патриотизме (USAPA).

В 2003 году Президентом США была утверждена «Национальная стратегия обеспечения безопасности киберпространства». Этот объемный документ адресован широкой общественности и направлен на расширение взаимодействия и консолидацию усилий различных слоев общества, государственных, общественных и частных организаций в деле противодействия кибертерроризму. Основная часть Стратегии расставляет приоритеты по созданию системы ответных мер, программы противодействия угрозам и уязвимостям,

программы обучения и повышения осведомленности, национальной и международной кооперации. Повышение защищенности промышленных систем было объявлено в США национальным приоритетом.

Российское правительство также начинает задумываться о защите государственного информационного пространства в сети Интернет. Начать, как водится, решено с разработки концепции. Когда эта концепция увидит свет пока сказать сложно.

Из новостей СМИ:

Правительство РФ всерьез задумалось о безопасности российского сегмента Интернета. Специальная рабочая группа при Минкомсвязи займется написанием концепции повышения безопасности Рунета, рассказал министр связи и массовых коммуникаций.

Направление работ и примерные меры по усилению безопасности Рунета министр не сообщил, однако среди существующих в нем угроз он назвал взломы и атаки, ограничивающие доступ к сайтам, в частности, коммерческих и правительственных учреждений.

Корпоративное управление

Законодательное и нормативное регулирование в области корпоративного управления нацелено на защиту инвесторов. Оно направлено главным образом на открытые акционерные общества и требует от них демонстрации должного усердия при раскрытии финансовой информации, прозрачного управления операционными рисками и реализации серии внутренних механизмов контроля и процедур, которые позволят этого добиться. Основной целью этих мер является убеждение потенциальных и существующих инвесторов в том, что финансовая отчетность бизнеса представляет правдивую картину организации, и они вполне могут на нее полагаться.

В Европе корпоративное управление регулируется такими нормативными актами, как Объединенные Правила внутреннего контроля (Turnbull), для компаний, акции которых котируются на Лондонской Фондовой Бирже (LSE); положение о контроле операционного риска в Базель II, для банков, участвующих в международной торговле; а также «Руководство для органов управления финансовыми сервисами (FSA)» для банков и финансовых организаций Объединенного Королевства. Контроль процессов аудита в Объединенном Королевстве стал частью законодательной базы с вводом в действие «Акта о компаниях» 2004 года.

В США Акт Сарбейнса-Оксли (SOX) поставил корпоративное управление на прочный законодательный фундамент, определив персональную ответственность руководства за предоставление недостоверной информации в финансовых отчетах, наказываемое тюремным заключением для главных исполнительных директоров (CEO) и главных финансовых директоров (CFO).

Риски подвергнуться предусмотренным законодательством санкциям за несоответствие SOX и Turnbull актуальны и для ряда российских компаний, акции которых торгуются на Нью-Йорской и Лондонской фондовых биржах. Эти компании, как правило, являются лидерами своих отраслей и активно привлекают зарубежные инвестиции на фондовом рынке.

Нормативное регулирование электронной коммерции

Целью законодательного и нормативного регулирования в области электронной коммерции является повышение доверия граждан к онлайновым транзакциям, которые становятся одним из важнейших механизмов в современной экономике. Для достижения этой цели разрабатываются требования по обеспечению безопасности информационных систем, используемых для реализации онлайновых транзакций.

Эти требования охватывают следующие области:

- использование электронных записей и электронных подписей;
- создание, модификация, хранение и передача электронных данных;
- предотвращение нецелевого использования ИТ систем.

Большинство европейских стран имеют законодательные акты, эквивалентные Акту о компьютерных злоупотреблениях Объединенного Королевства. ЕС активно формирует законодательную базу в этой области, примеры которой включают:

- Директиву об электронных подписях;
- Директиву о защите потребителей и дистанционных продажах;
- Директиву о защите персональных данных и электронных коммуникаций;
- Конвенцию Совета Европы о киберпреступности.

США менее активны в данной области. Их законотворчество носит отраслевой характер. Например, существуют Положения об администрировании продуктов питания и лекарственных препаратов (FDA), регулирующие использование электронных записей и подписей в фармацевтической промышленности (21CFR11). Комиссия по ценным бумагам и фондовым биржам (SEC) проявляла определенную активность в области управления жизненным циклом документов и предложила ряд федеральных нормативных актов США, которые были приняты в нескольких штатах.

Защита персональных данных

Законодательное и нормативное регулирование в области защиты персональных данных предназначено для определения прав и обязанностей физических лиц и организаций применительно к сбору, использованию, сохранению и раскрытию персональных данных. В случае неправомерного раскрытия требуется извещение.

В Европейском Союзе все страны ввели в действие национальное

законодательство на базе Директивы Европейского Союза о защите данных.

Канада приняла подход, аналогичный принятому в Европейском Союзе Акту о защите персональной информации и электронных документов (PIPEDA).

Законодательство США по защите персональных данных направлено на *конкретные области*, такие как:

- Акт Грэмм-Лич-Блайли (GLBA);
- Акт об учете и страховании здоровья (HIPAA)

или оно ориентировано на *конкретные типы преступлений*, например:

- Акт Калифорнии о нарушении безопасности информации (Билль Сената № 1386) (ориентирован на кражу персональных данных);
- Акт о защите частной жизни детей в онлайне (COPPA);
- Акт о правах семей на образование и частную жизнь (FERPA).

Законодательство США предусматривает очень серьезное наказание за раскрытие персональных данных граждан. Соответствующие вопросы отражены в Privacy Act и HIPPA. Последний определяет наказание до 10 лет лишения свободы или 200 тыс. долларов штрафа за умышленное раскрытие персональных данных.

Принятый в июле 2006 года в России закон «О персональных данных» (ФЗ-152) внес еще больше сумятицы и в без того непростую ситуацию с законодательством в сфере защиты информации. Предоставленная операторам персональных данных отсрочка по выполнению требований этого закона действует до 2010 года, и организациям приходится принимать экстренные меры, чтобы не подвергать себя рискам применения к ним санкций со стороны государства.

Меры эти заключаются в выполнении весьма нетривиальных требований закона и выпущенных на его основе нормативных актов, а именно:

- Регистрация в качестве оператора персональных данных в Россвязькомнадзоре.
- Разработка и принятие документов, регламентирующих вопросы предоставления доступа и защиты персональных данных, оформления допусков сотрудников к этим данным.
- Формирование перечня обрабатываемых персональных данных, классификация информационных систем персональных данных (ИСПД) и подготовка этих систем к аттестации по требованиям безопасности, что влечет за собой также сертификацию средств защиты информации (СЗИ) и средств обработки информации (СОИ), используемых в составе ИСПД.
- Операторам ИСПД первого и второго класса, согласно устанавливаемой в нормативных документах ФСТЭК классификации, кроме того, предписывается получать лицензии ФСТЭК на осуществление деятельности по технической защите конфиденциальной информации (ТЗКИ) либо отдавать обслуживание таких систем на аутсорсинг лицензиатам ФСТЭК.

Прежде всего возникает вопрос, а возможно ли вообще на практике обеспечить выполнение требований данного закона? Например, для выполнения требования о регистрации операторов персональных данных необходимо как минимум провести всероссийскую перепись населения и юридических лиц! Ведь, согласно определению Закона, оператор ПД – это «государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных». Под персональными данными понимается «любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу», а под обработкой ПД понимаются любые действия с ними, включая их хранение.

У каждого из нас в мобильном телефоне имеется база персональных данных, обрабатываемая с использованием средств автоматизации. База персональных данных по клиентам и контрагентам имеется также у любой организации. Если руководствоваться принятыми определениями, то в России насчитываются десятки миллионов операторов персональных данных, которые должны быть зарегистрированы надлежащим образом в Россвязькомнадзоре. Непонятно, каким образом будет выполняться данное требование закона. В конечном счете государственные контролирующие органы сами будут решать, к кому применять, а к кому не применять нормы закона.

Забота государства о своих гражданах и их конституционных правах понятна и обоснована. Однако на деле все в основном сводится к выписыванию бумажек (лицензий, сертификатов и аттестатов), которые обходятся весьма недешево, но на практике защищают не персональные данные граждан, а лишь обладателей этих бумажек от возможных «наездов», создавая дополнительный фронт работ для тех, кто эти бумажки выписывает. Если раньше аттестация АС носила добровольный характер для большинства негосударственных организацией, то теперь почти в каждой организации можно найти объекты, подлежащие обязательной аттестации. Эта ситуация будет способствовать избирательности применения данных норм и их свободной трактовке как со стороны регулирующих органов, так и со стороны тех, кому предписано эти нормы выполнять. В результате, как обычно, получаем перекладывание денег из одних карманов в другие.

В отношении ФЗ-152 сейчас раздается много критики со всех сторон. Но ведь РФ не является первооткрывательницей в вопросах защиты информации и персональных данных в частности. Многое заимствуется из европейского и американского законодательства, которое ушло в своем развитии далеко вперед. Британский Акт о защите данных (UK Data Protection Act) был принят еще в 1984 году, а затем обновлен в 1998 году, после выхода директивы Европейского Союза о защите данных (EU Directive on Data Protection). Не удивительно,

что ФЗ-152 принципиально мало чем отличается от европейских законодательных актов. Если не углубляться в юридические тонкости, то фактически тем же самым принципам в защите персональных данных следуют все европейские страны.

Европейское законодательство также предусматривает обязательную регистрацию операторов персональных данных, сталкиваясь при этом с теми же самыми проблемами. Исследование, проведенное Personnel Policy Research Unit в 1998 году (через 14 лет после принятия Британского Закона о защите данных) показало, что из 1100 опрошенных ИТ менеджеров 19% вообще не имеют понятия о требовании по регистрации в качестве оператора ПД, а в небольших компаниях таких ИТ менеджеров 48%. Кроме этого, 48% опрошенных в крупных компаниях и 66% в малом бизнесе затруднились ответить на вопрос об обязанностях оператора в отношении обеспечения безопасности ПД. Только 1% опрошенных вспомнили о том, что передача ПД должна оформляться должным образом и 2% вспомнили, что ПД не должны храниться дольше, чем требуется. Британский Реестр персональных данных (Data Protection Register) в 1998 году содержал более 200 тыс. записей об операторах и каждую неделю там регистрировалось еще 500 операторов. Пятая часть компаний к этому времени еще не выполнили требования о регистрации.

Европейская директива 1998 года предоставила операторам ПД еще до 12 лет отсрочки в отношении выполнения ряда требований. Российская четырехлетняя отсрочка закончится в 2010 году, одновременно с их двенадцатилетней отсрочкой. Как видим, наши операторы ПД поставлены в значительно более жесткие условия, нежели европейские, обладающие форой в более чем 20 лет.

Обращает на себя внимание разница между европейским и в российским законодательством в определении ключевого понятия – «персональные данные». Согласно ФЗ-152: «персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), **в том числе его фамилия, имя,**

отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация».

Европейское определение ПД звучит следующим образом: «**персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных)** ***и включающая в себя любое выражение мнения об индивидууме и любые признаки намерения оператора данных или любого другого лица в отношении индивидуума»,*** а вовсе не имя, фамилия, отчество, адрес и т.п., как в российском варианте.

Другими словами, европейские законодатели считают персональными данными не то же самое, что российские. Европейские ПД – это лишь подмножество российских ПД. И хотя такие понятия, как «выражение мнения» и «признаки намерения» явно нуждаются в дальнейшем разъяснении, очевидно, что к ПД в Европе вряд ли можно отнести, например, рабочие контакты, хранящиеся в мобильных телефонах (ФИО, номер телефона, адрес и название компании, где человек работает).

России предстоит пройти еще долгий путь совершенствования законодательства в области персональных данных и формирования соответствующей правоприменительной практики.

Защита интеллектуальной собственности

Все страны используют определенные формы законодательства о коммерческой тайне, авторском праве и патентах, направленного на защиту интеллектуальной собственности физических лиц и организаций. В России вопросы защиты прав интеллектуальной собственности регулируются четвертой частью Гражданского Кодекса РФ.

Наибольшее значение для организаций имеет обеспечение защиты коммерческой тайны. Предметом защиты коммерческой информации являются все, свойственные предприятиям компании особенности и детали коммерческой деятельности, деловые связи, закупка сырья

и товаров, сведения о поставщиках, предполагаемой прибыли, методики установления цен, результаты маркетинговых исследований, счета, договора и т.п.

По гражданскому законодательству (ст. 139 Гражданского Кодекса РФ) обладатель технической, организационной или коммерческой информации, составляющей секрет производства, имеет правовую защиту от незаконного ее использования при условии, что:

- эта информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам;
- к этой информации нет свободного доступа на законном основании;
- обладатель информации принимает надлежащие меры к соблюдению ее конфиденциальности.

Отношения, возникающие между субъектами гражданского общества, связанные с отнесением информации к коммерческой тайне, передачей такой информации, и охраной ее конфиденциальности, регулируются Законом РФ «О коммерческой тайне», согласно которому права обладателя информации, составляющей коммерческую тайну, возникают с момента установления им в отношении такой информации режима коммерческой тайны, под которым понимаются «правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности».

Отраслевая специфика

Отраслевая нормативная база предназначена для контроля тех аспектов информационной безопасности, которые являются уникальными для определенной отрасли и от которых зависит ее безопасность или безопасность широкой общественности. Примеры из европейского законодательства включают в себя нормативные документы Управления питания и фармацевтики (FDA) для фармацевтических компаний, а также законы о сохранении данных,

которые действуют в отношении телекоммуникационных и Интернет провайдеров. Нормативные акты, применимые к компаниям, выпускающим кредитные карты, также применяются и к организациям, имеющими дело с этими компаниями.

Развитие российского рынка ИБ в немалой степени связано с возрастанием требований по ИБ в таких монополистах, как Банк России, РЖД, система электроэнергетики (бывшая РАО ЕЭС), Газпром и пр., пытающихся сформировать собственную отраслевую нормативную базу в области ИБ для подконтрольных им структур. Например, в Банке России введен в действие ряд стандартов по ИБ, которые пока носят рекомендательный характер, но в дальнейшем вполне могут стать обязательными.

Организации должны определить какие отраслевые нормативные акты применимы в их юрисдикции и учитывать их при оценке юридических рисков, связанных с невыполнением требований информационной безопасности.